

In the Claims

1. (Original) A method comprising:
creating a data structure including a plurality of user id-user key pairs, each user id-user key pair comprising a user id associated with one of a plurality of users and a user key comprising a master key encrypted using a password associated with the one of the plurality of users; and
delivering the data structure to one or more of the plurality of users.
2. (Original) A method as recited in claim 1, wherein the act of delivering comprises delivering the data structure to each of the plurality of users.
3. (Original) A method as recited in claim 1, wherein each master key is encrypted using a hash of the password associated with the one of the plurality of users.
4. (Original) A method as recited in claim 1, wherein each master key is encrypted using a one-way hash of the password associated with the one of the plurality of users.
5. (Original) A method as recited in claim 1, wherein each master key is encrypted using a cryptographic hash of the password associated with the one of the plurality of users.

1 6. (Original) A method as recited in claim 1, wherein each user key
2 has an integrity verification feature associated therewith.

3
4 7. (Original) A method as recited in claim 1, wherein each master key
5 has an integrity verification feature associated therewith.

6
7 8. (Original) A method as recited in claim 1, wherein each master key
8 and each master key has an integrity verification feature associated therewith.

9
10 9. (Original) A method as recited in claim 1, wherein each user key
11 includes a checksum.

12
13 10. (Original) A method as recited in claim 1, wherein each user key
14 includes a keyed-hash message authentication code.

15
16 11. (Original) A method as recited in claim 1, further comprising:
17 transforming data using the master key.

18
19 12. (Original) A method as recited in claim 1, further comprising:
20 storing data transformed using the master key; and
21 controlling access by the plurality of users to the transformed data.

1 13. (Original) A method as recited in claim 1, further comprising:
2 storing data transformed using the master key;
3 receiving a user id and user password from one of the plurality of users; and
4 controlling access to the transformed data by the one of the plurality of
5 users based on the received user id and user password.

6
7 14. (Original) A method as recited in claim 1, further comprising:
8 storing data transformed using the master key;
9 receiving a user id and user password from one of the plurality of users; and
10 accessing the transformed data using the received user id and user
11 password.

12
13 15. (Original) A method as recited in claim 1, further comprising:
14 storing data transformed using the master key;
15 receiving a user id and user password from one of the plurality of users;
16 selecting a user key from the data structure based on the received user id;
17 decrypting the selected user id using the received password to reproduce the
18 master key; and
19 using the master key to access the data.
20
21
22
23
24
25

1 16. (Original) A method as recited in claim 1, further comprising:
2 storing data watermarked using the master key;
3 receiving a user id and user password from one of the plurality of users; and
4 selecting a user key from the data structure based on the received user id;
5 hashing the received password to produce a hash value;
6 decrypting the selected user id using the hash value to reproduce the master
7 key; and
8 using the master key to access the watermarked data.

9
10 17. (Withdrawn) A method comprising:
11 retrieving a user key associated with a first user of a plurality of users from
12 a data structure comprising a plurality of user keys, each user key comprising a
13 master key encrypted using a password associated with a unique one of the
14 plurality of users;
15 decrypting the retrieved user key using a password associated with the first
16 user to produce a master key; and
17 accessing data using the master key.

18
19 18. (Withdrawn) A method as recited in claim 17, wherein the user key
20 is retrieved using a user id associated with the first user.
21
22
23
24
25

1 19. (Withdrawn) A method as recited in claim 17, wherein the data
2 structure comprises a plurality of user id-user key pairs, each user id-user key pair
3 comprising a user id associated with one of a plurality of users and a user key
4 associated with the one of the plurality of users.

5
6 20. (Withdrawn) A method as recited in claim 17, wherein the data
7 structure comprises a plurality of user id-user key pairs, each user id-user key pair
8 comprising a user id associated with one of a plurality of users and a user key
9 associated with the one of the plurality of users, and wherein the user key is
10 retrieved using a user id associated with the first user.

11
12 21. (Withdrawn) A method as recited in claim 17, wherein the act of
13 decrypting the user key comprises decrypting the user key using a hash of the
14 password associated with the first user.

15
16 22. (Withdrawn) A method as recited in claim 17, wherein the act of
17 decrypting the retrieved user key comprises:

18 hashing the password associated with the first user to produce a hash value;

19 and

20 using the hash value as a decryption key to decrypt the user key.
21
22
23
24
25

1
2 23. (Withdrawn) A method as recited in claim 17, wherein the act of
3 decrypting the retrieved user key comprises:

4 hashing the password associated with the first user using a one-way hash
5 function; and

6 using the result of the one-way hash function as a decryption key to decrypt
7 the user key.

8
9 24. (Withdrawn) A method as recited in claim 17, wherein the act of
10 decrypting the retrieved user key comprises:

11 hashing the password associated with the first user using a cryptographic
12 hash function; and

13 using the result of the cryptographic hash function as a decryption key to
14 decrypt the user key.

15
16 25. (Withdrawn) A method as recited in claim 17, wherein each of the
17 plurality of user keys includes a data verification feature.

18
19 26. (Withdrawn) A method as recited in claim 17, wherein each of the
20 plurality of master keys includes a data verification feature.

21
22 27. (Withdrawn) A method as recited in claim 17, further comprising:
23 verifying the integrity of the retrieved user key.
24
25

1 28. (Withdrawn) A method as recited in claim 17, wherein the retrieved
2 user key includes an integrity verification feature and wherein the method further
3 comprises verifying the integrity of the retrieved user key using the integrity
4 verification feature.

5
6 29. (Withdrawn) A method as recited in claim 17, wherein the retrieved
7 user key includes a checksum and wherein the method further comprises verifying
8 the integrity of the retrieved user key using the checksum.

9
10 30. (Withdrawn) A method as recited in claim 17, wherein the retrieved
11 user key includes a message authentication code and wherein the method further
12 comprises verifying the integrity of the retrieved user key using the message
13 authentication code.

14
15 31. (Withdrawn) A method as recited in claim 17, wherein the retrieved
16 user key includes a keyed-hash message authentication code and wherein the
17 method further comprises verifying the integrity of the retrieved user key using the
18 keyed-hash message authentication code.

1 32. (Original) A computer readable medium having stored thereon a
2 data structure comprising:

3 a plurality of user id-user key pairs, each user id-user key pair comprising a
4 user id associated with one of a plurality of users and a user key comprising a
5 master key encrypted using a password associated with the one of the plurality of
6 users.

7
8 33. (Original) A computer readable medium as recited in claim 32,
9 wherein each user key comprises a master key encrypted using a hash of the
10 password associated with the one of the plurality of users.

11
12 34. (Original) A computer readable medium as recited in claim 32,
13 wherein each user key comprises a master key encrypted using a one-way hash of
14 the password associated with the one of the plurality of users.

15
16 35. (Original) A computer readable medium as recited in claim 32,
17 wherein each user key comprises a master key encrypted using a cryptographic
18 hash of the password associated with the one of the plurality of users.

19
20 36. (Original) A computer readable medium as recited in claim 32,
21 wherein each user key includes an integrity verification feature.

22
23 37. (Original) A computer readable medium as recited in claim 32,
24 wherein each master key includes an integrity verification feature.
25

1
2 38. (Original) A computer readable medium as recited in claim 32,
3 wherein each user key includes a checksum.
4

5 39. (Original) A computer readable medium as recited in claim 32,
6 wherein each user key includes a keyed-hash message authentication code.
7

8 40. (Withdrawn) A system comprising:
9 a hashing module operable to hash each of a plurality of user passwords
10 to produce a plurality of hash values;
11 an encryption module operable to create a plurality of user keys, each
12 user key comprising a master key encrypted using one of the hash values as an
13 encryption key; and
14 a data structure creation module operable to associate each of the user
15 keys with a user id in a data structure.
16

17 41. (Withdrawn) A system as defined in claim 40, wherein the
18 hashing module produces the hash values using a one-way hashing function.
19

20 42. (Withdrawn) A system as defined in claim 40, wherein the
21 hashing module produces the hash values using a cryptographic hashing
22 function.
23
24
25

1 43. (Withdrawn) A system as defined in claim 40, wherein the data
2 structure creation module associates each user key with a user id in a user id-
3 user key pair, and wherein each user id-user key pair is associated with a single
4 user.

5
6 44. (Withdrawn) A system as defined in claim 40, wherein the
7 encryption module includes an integrity verification feature in each user key.

8
9 45. (Withdrawn) A system as defined in claim 40, wherein the
10 encryption module includes a checksum in each user key.

11
12 46. (Withdrawn) A system as defined in claim 40, wherein the
13 encryption module includes a message authentication code in each user key.

14
15 47. (Withdrawn) A system as defined in claim 40, wherein the
16 encryption module includes a keyed-hash message authentication code in each
17 user key.

1 48. (Withdrawn) A system comprising:

2 a user key data structure including plurality of user id-user key pairs,
3 each user key pair including a user key and a user id associated with one of a
4 plurality of users, each user key comprising an encrypted version of a common
5 master key;

6 a master key decryption module operable to select a user key from the
7 user key data structure based on a user id received from one of the plurality of
8 users and to decrypt the selected user key using a password received from the
9 one of the plurality of users.

10
11 49. (Withdrawn) A system as recited in claim 48, further comprising
12 a data decryption module operable to decrypt data encrypted using the master
13 key as an encryption key.

14
15 50. (Withdrawn) A system as recited in claims 48, further comprising
16 an error handler module operable to indicate to the one of the plurality when an
17 error occurs in decrypting the user key.

1 51. (Withdrawn) A system as recited in claims 48, wherein the master
2 key decryption module comprises:

3 a hashing module operable to hash a password received from the one of
4 the plurality of users to produce a hash value; and

5 a user key decryption module operable to select a user key from the user
6 key data structure based on a user id received from one of the plurality of users
7 and to decrypt the selected user key using the hash value as a decryption key.

8
9 52. (Withdrawn) A system as recited in claims 48, wherein the master
10 key decryption module comprises:

11 a hashing module operable to hash a password received from the one of
12 the plurality of users using a one-way hashing function to produce a hash value;
13 and

14 a user key decryption module operable to select a user key from the user
15 key data structure based on a user id received from one of the plurality of users
16 and to decrypt the selected user key using the hash value as a decryption key.

1 53. (Withdrawn) A system as recited in claim 48, wherein the master
2 key decryption module comprises:

3 a hashing module operable to hash a password received from the one of
4 the plurality of users using a cryptographic hashing function to produce a hash
5 value; and

6 a user key decryption module operable to select a user key from the user
7 key data structure based on a user id received from one of the plurality of users
8 and to decrypt the selected user key using the hash value as a decryption key.

9
10 54. (Withdrawn) A system as recited in claims 48, wherein the master
11 key decryption module comprises:

12 a hashing module operable to hash a password received from the one of
13 the plurality of users to produce a hash value; and

14 a user key decryption and integrity module operable to select a user key
15 from the user key data structure based on a user id received from one of the
16 plurality of users, to confirm the integrity of the selected user id, and to decrypt
17 the selected user key using the hash value as a decryption key.

1 55. (Withdrawn) A system as recited in claims 48, wherein each user
2 key in the user key data structure includes an integrity verification feature, and
3 wherein the master key decryption module comprises:

4 a hashing module operable to hash a password received from the one of
5 the plurality of users to produce a hash value; and

6 a user key decryption and integrity module operable to select a user key
7 from the user key data structure based on a user id received from one of the
8 plurality of users, to confirm the integrity of the selected user id using the
9 integrity verification feature included in the user key, and to decrypt the selected
10 user key using the hash value as a decryption key.

11
12 56. (Original) A system comprising:

13 means for producing a user key associated with each of a plurality users,
14 each user key comprising a master key encrypted using a password of the one
15 of the plurality of users associated with the user key;

16 means for associating each of the user keys with a user id of the one of
17 the plurality of users associated with the user key in a data structure.

18
19 57. (Original) A computer-readable medium having stored thereon
20 computer executable instructions for performing acts of:

21 creating a data structure including a plurality of user id-user key pairs, each
22 user id-user key pair comprising a user id associated with one of a plurality of
23 users and a user key comprising a master key encrypted using a password
24 associated with the one of the plurality of users.

1
2 58. (Original) A computer-readable medium as recited in claim 57
3 having further computer executable instructions for performing acts of:
4 delivering the data structure to one or more of the plurality of users.
5

6 59. (Original) A computer-readable medium as recited in claim 57
7 having further computer executable instructions for performing acts of:
8 delivering the data structure to each of the plurality of users.
9

10 60. (Original) A computer-readable medium as recited in claim 57,
11 wherein each master key is encrypted using a hash of the password associated with
12 the one of the plurality of users.
13

14 61. (Original) A computer-readable medium as recited in claim 57,
15 wherein each master key is encrypted using a one-way hash of the password
16 associated with the one of the plurality of users.
17

18 62. (Original) A computer-readable medium as recited in claim 57,
19 wherein each master key is encrypted using a cryptographic hash of the password
20 associated with the one of the plurality of users.
21

22 63. (Original) A computer-readable medium as recited in claim 57,
23 wherein each user key has an integrity verification feature associated therewith.
24
25

1
2 64 (Original) A computer-readable medium as recited in claim 57,
3 wherein each user key includes a checksum.
4

5 65. (Original) A computer-readable medium as recited in claim 57,
6 wherein each user key includes a keyed-hash message authentication code.
7

8 66. (Original) A computer-readable medium as recited in claim 57
9 having further computer executable instructions for performing acts of:
10 transforming data using the master key.
11

12 67. (Original) A computer-readable medium as recited in claim 57
13 having further computer executable instructions for performing acts of:
14 storing data transformed using the master key; and
15 controlling access by the plurality of users to the transformed data.
16

17 68. (Original) A computer-readable medium as recited in claim 57
18 having further computer executable instructions for performing acts of:
19 storing data transformed using the master key;
20 receiving a user id and user password from one of the plurality of users; and
21 controlling access to the transformed data by the one of the plurality of
22 users based on the received user id and user password.
23
24
25

1 69. (Original) A computer-readable medium as recited in claim 57
2 having further computer executable instructions for performing acts of:
3 storing data encrypted using the master key;
4 receiving a user id and user password from one of the plurality of users; and
5 accessing the transformed data using the received user id and user
6 password.

7
8 70. (Original) A computer-readable medium as recited in claim 57
9 having further computer executable instructions for performing acts of:
10 storing data encrypted using the master key;
11 receiving a user id and user password from one of the plurality of users;
12 selecting a user key from the data structure based on the received user id;
13 decrypting the selected user id using the received password to reproduce the
14 master key; and
15 using the master key to decrypt the data.

1 71. (Original) A computer-readable medium as recited in claim 57
2 having further computer executable instructions for performing acts of:

3 storing data watermarked using the master key;

4 receiving a user id and user password from one of the plurality of users; and

5 selecting a user key from the data structure based on the received user id;

6 hashing the received password to produce a hash value;

7 decrypting the selected user id using the hash value to reproduce the master
8 key; and

9 using the master key to access the watermarked data.

10 72. (Withdrawn) A computer-readable medium having stored thereon
11 computer executable instructions for performing acts of:
12

13 retrieving a user key associated with a first user of a plurality of users from
14 a data structure comprising a plurality of user keys, each user key comprising a
15 master key encrypted using a password associated with a unique one of the
16 plurality of users;

17 decrypting the retrieved user key using a password associated with the first
18 user to produce a master key; and
19

20 accessing data using the master key.

21
22 73. (Withdrawn) A computer-readable medium as recited in claim 72,
23 wherein the user key is retrieved using a user id associated with the first user.
24
25

1 74. (Withdrawn) A computer-readable medium as recited in claim 72,
2 wherein the data structure comprises a plurality of user id-user key pairs, each user
3 id-user key pair comprising a user id associated with one of a plurality of users
4 and a user key associated with the one of the plurality of users.

5
6 75. (Withdrawn) A computer-readable medium as recited in claim 72,
7 wherein the data structure comprises a plurality of user id-user key pairs, each user
8 id-user key pair comprising a user id associated with one of a plurality of users
9 and a user key associated with the one of the plurality of users, and wherein the
10 user key is retrieved using a user id associated with the first user.

11
12 76. (Withdrawn) A computer-readable medium as recited in claim 72,
13 wherein the act of decrypting the user key comprises decrypting the user key using
14 a hash of the password associated with the first user.

15
16 77. (Withdrawn) A computer-readable medium as recited in claim 72,
17 wherein the act of decrypting the retrieved user key comprises:

18 hashing the password associated with the first user to produce a hash value;

19 and

20 using the hash value as a decryption key to decrypt the user key.
21
22
23
24
25

1
2 78. (Withdrawn) A computer-readable medium as recited in claim 72,
3 wherein the act of decrypting the retrieved user key comprises:

4 hashing the password associated with the first user using a one-way hash
5 function; and

6 using the result of the one-way hash function as a decryption key to decrypt
7 the user key.

8
9 79. (Withdrawn) A computer-readable medium as recited in claim 72,
10 wherein the act of decrypting the retrieved user key comprises:

11 hashing the password associated with the first user using a cryptographic
12 hash function; and

13 using the result of the cryptographic hash function as a decryption key to
14 decrypt the user key.

15
16 80. (Withdrawn) A computer-readable medium as recited in claim 72,
17 wherein each of the plurality of user key includes a data verification feature.

18
19 81. (Withdrawn) A computer-readable medium as recited in claim 72
20 having further computer executable instructions for performing acts of:
21 verifying the integrity of the retrieved user key.
22
23
24
25

1 82. (Withdrawn) A computer-readable medium as recited in claim 72,
2 wherein the retrieved user key includes an integrity verification feature and
3 wherein the method further comprises verifying the integrity of the retrieved user
4 key using the integrity verification feature.

5
6 83. (Withdrawn) A computer-readable medium as recited in claim 72,
7 wherein the retrieved user key includes a checksum and wherein the method
8 further comprises verifying the integrity of the retrieved user key using the
9 checksum.

10
11 84. (Withdrawn) A computer-readable medium as recited in claim 72,
12 wherein the retrieved user key includes a message authentication code and
13 wherein the method further comprises verifying the integrity of the retrieved user
14 key using the message authentication code.

15
16 85. (Withdrawn) A computer-readable medium as recited in claim 72,
17 wherein the retrieved user key includes a keyed-hash message authentication code
18 and wherein the method further comprises verifying the integrity of the retrieved
19 user key using the keyed-hash message authentication code.
20
21
22
23
24
25